



CENTER FOR ENTERPRISE MODERNIZATION

Information Sharing Risk Assessment: The RAISE Methodology

Deb Bodeau

Don Faatz

Rich Graubart

2007

Approved for Public Release; Distribution Unlimited
Case # 07-1376

© 2007 The MITRE Corporation
All rights reserved

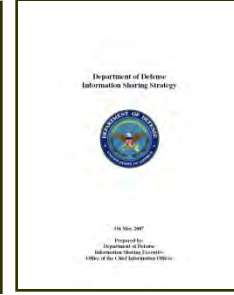
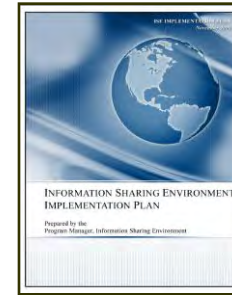


Executive Summary

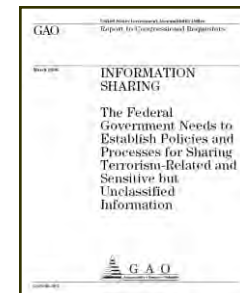
- The information sharing problem domain is large and complex
- The RAISE methodology provides a risk-based approach to navigating this domain
- RAISE includes
 - A framework of information sharing goals and capabilities
 - A model of information sharing situations that
 - ❖ Represents stakeholder concerns and incentives
 - ❖ Captures risk factors related to security, criticality, and stakeholder relationships
 - ❖ Recommends risk-appropriate levels of capabilities
 - A proof-of-concept tool that automates portions of the model
 - A process for using the framework, model, and tool
- RAISE Version 1.0 is available for use

Information Sharing: Easy to Demand, Hard to Achieve

- Many assert the need for better information sharing
 - To support missions with timely, decision-supportive information
 - To improve efficiency and lower costs



- Many technologies are presented as information sharing solutions, but are not complete solutions
 - Enabling technologies from many domains, including information security, information management
 - Provide specific capabilities, assuming specific technical environments ... so do not address sharing of hardcopy or sharing via face-to-face interactions
 - Do not address social / organizational processes

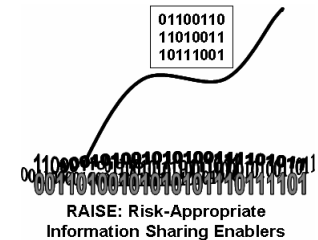


- Cultural and policy obstacles impede adoption of technologies



RAISE: A Structured Approach to Information Sharing Risk Management

- RAISE: Risk-Appropriate Information Sharing Enablers
- Overarching goal: Facilitate management of information sharing risks
- Observations regarding risks and risk management motivate the RAISE approach
- RAISE includes
 - A framework of information sharing goals and capabilities
 - An information sharing risk model
 - A proof-of-concept tool that automates portions of the model
 - A process for using the framework, model, and tool



Motivating Observations about Risk

- Risks arise from not sharing (or from ineffective sharing) as well as from sharing information
- Risks are experienced by, and risk management decisions are distributed among, a variety of stakeholders
 - Stakeholders include
 - ❖ Participants in information sharing: information providers, recipients, and those who provide venues in which information may be shared (“venue stewards”)
 - ❖ Those who benefit (directly or indirectly) from information sharing, notably mission or business process owners
 - ❖ Other interested parties: information owners (e.g., for entertainment content), information subjects if personal information is shared, oversight bodies, etc.
 - Decisions can include policy mandates or prohibitions, agreement or refusal to participate, use of specific enabling technologies or processes
- Risks must thus be managed holistically rather than in isolation
 - Support for risk management is provided by policy advisors, systems / business process engineers, and researchers / developers



RAISE Goal: Facilitate Management of Information Sharing Risks

- Enable policy advisors to
 - Broker negotiations among stakeholders with different concerns, incentives, and priorities
 - Articulate information sharing goals and strategies for meeting those goals
- Enable systems / business process engineers to
 - Specify capabilities needed to mitigate information sharing risks
 - Determine whether specific technologies or processes will provide needed capabilities
- Help researchers and developers to
 - Situate their efforts: which parts of the information sharing problem do they address?
 - Identify and meet needs: what capability gaps remain?



RAISE Overview

RAISE Framework	Goal Priority Model	<ul style="list-style-type: none"> • Identify, describe, or characterize an information sharing situation <ul style="list-style-type: none"> • Identify the information to be shared • Describe the reason(s) for sharing information • Identify stakeholders <ul style="list-style-type: none"> • Information provider • Information recipient • Information subject • Interested parties (Information owner, Mission owner, Information sharing venue steward, Other interested parties) • Collect prioritized concerns and incentives related to sharing information from each stakeholder • Map stakeholder concerns and incentives to prioritized information sharing goals 	RAISE Tool
	RESULT	<ul style="list-style-type: none"> • Stakeholders clearly understand the benefits and risks of information sharing 	
	Risk-Appropriate Capability Model	<ul style="list-style-type: none"> • RAISE defines capabilities that can be used to achieve information sharing goals • Risk factors associated with capabilities are assigned levels (e.g., High, Medium) • RAISE functions map risk factor levels to the associated capability levels needed to achieve information sharing goals • RAISE recommends a prioritized set of capabilities that mitigate stakeholder concerns and achieve information sharing goals • Stakeholders review RAISE recommendations and reach agreement on required capabilities • Mechanisms are chosen to implement the required capabilities 	
	RESULT	<ul style="list-style-type: none"> • Risk-appropriate information sharing occurs 	

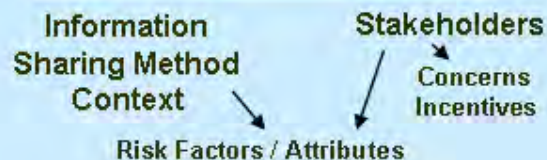


RAISE Framework

- Four overarching principles
 - Balance risks
 - Share effectively
 - Respect terms of use
 - Ensure accountability
- Twenty information sharing goals
- Forty-one capabilities to achieve those goals
 - Capabilities defined in a technology-neutral way, to accommodate all forms of information sharing
 - Capability levels ranging from None to High
- An enabling technology, process, or product provides one or more capabilities, at an assessable level (or levels)
- Capabilities can be assessed for an existing information sharing situation ... thus indicating how well various goals are being achieved

RAISE Goal Priority Model

Model Information Sharing Situation



Describe Information Sharing Principles and Goals

Balance Incentives and Risks:

- Engage stakeholders.
- Identify potential harms and benefits.
- Identify terms of use.
- Prevent unintended sharing.

Share Effectively:

- Share predictably.
- Share dynamically.
- Authorize initial disclosure.
- Make information understandable.
- Ensure quality.

Respect Terms of Use:

- Authorize additional sharing.
- Enable revocation.
- Provide corrections.
- Restrict uses.
- Protect information.
- Dispose of information.

Ensure Accountability:

- Give credit.
- Provide feedback.
- Steward sharing venues.
- Monitor information sharing actions.
- Redress violations.

Goal	Importance to Provider	Importance to Recipient	Importance to Venue Steward	Importance to Mission Owner
Engage stakeholders	Medium	Medium	None	High
Identify potential harms and benefits	High	Medium	None	High
Identify Terms of Use	None	Medium	None	Medium
Share predictably	Low	None	None	Medium
Share dynamically	Very Low	Medium	None	Medium
Authorize initial disclosure	High	Medium	None	High
Make information understandable	Very Low	None	None	Medium
Ensure quality	Very Low	None	None	-
Authorize additional sharing	High	None	None	None

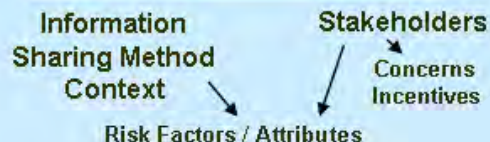
Assess Relative Priorities of Information Sharing Principles and Goals Highlight Differences among Stakeholders

This High-Level Model Enables Policy Advisors to Support Mission / Business Leaders:

- Represent concerns / incentives
- Highlight different priorities to help broker negotiation
- Provide a basis for policy and strategic planning

RAISE Risk-Appropriate Capability Model

Model Information Sharing Situation



Information Sharing Goal: Authorize Disclosure		
Capability	Achievement Levels / Values	Examples
Redaction: How completely and effectively is information that has not been authorized for disclosure or release as part of information sharing removed from a shared information object?	None – No attempt is made to identify and remove information that is not immediately apparent to the reviewer.	None
	Low – Unstructured processes to identify and remove information that is not immediately apparent are applied.	In Microsoft Office, the reviewer edits the document properties, accepts all changes, and saves the file as new.
	Medium – Partially structured processes are applied. Tools are matched to some types of shared information objects; if no tools are available for a given object type, ad-hoc analysis is performed.	Hidden data detection tools for documents
	High – Structured processes are applied. Sophisticated tools are matched to each type of information object that is shared.	Steganographic detection tools for images

Security Redaction				
Expected Degree of Information Transience	Provider-Recipient Authorization Difference			
	None	Low	Medium	High
Transient	None	None	None	Low
Delayed	None	None	Low	Medium
Persistent	None	Low	Medium	High
Privacy Redaction				
Expected Degree of Information Transience = Persistent and	Information Subject Privacy Concern (max(SS4, SS5, SS6))			
	None	Low	Medium	High
Information Type = PII	None	None	Low	Medium
Information Type = PHI	High			
Recommended Level of Redaction = max (Security Redaction, Privacy Redaction)				

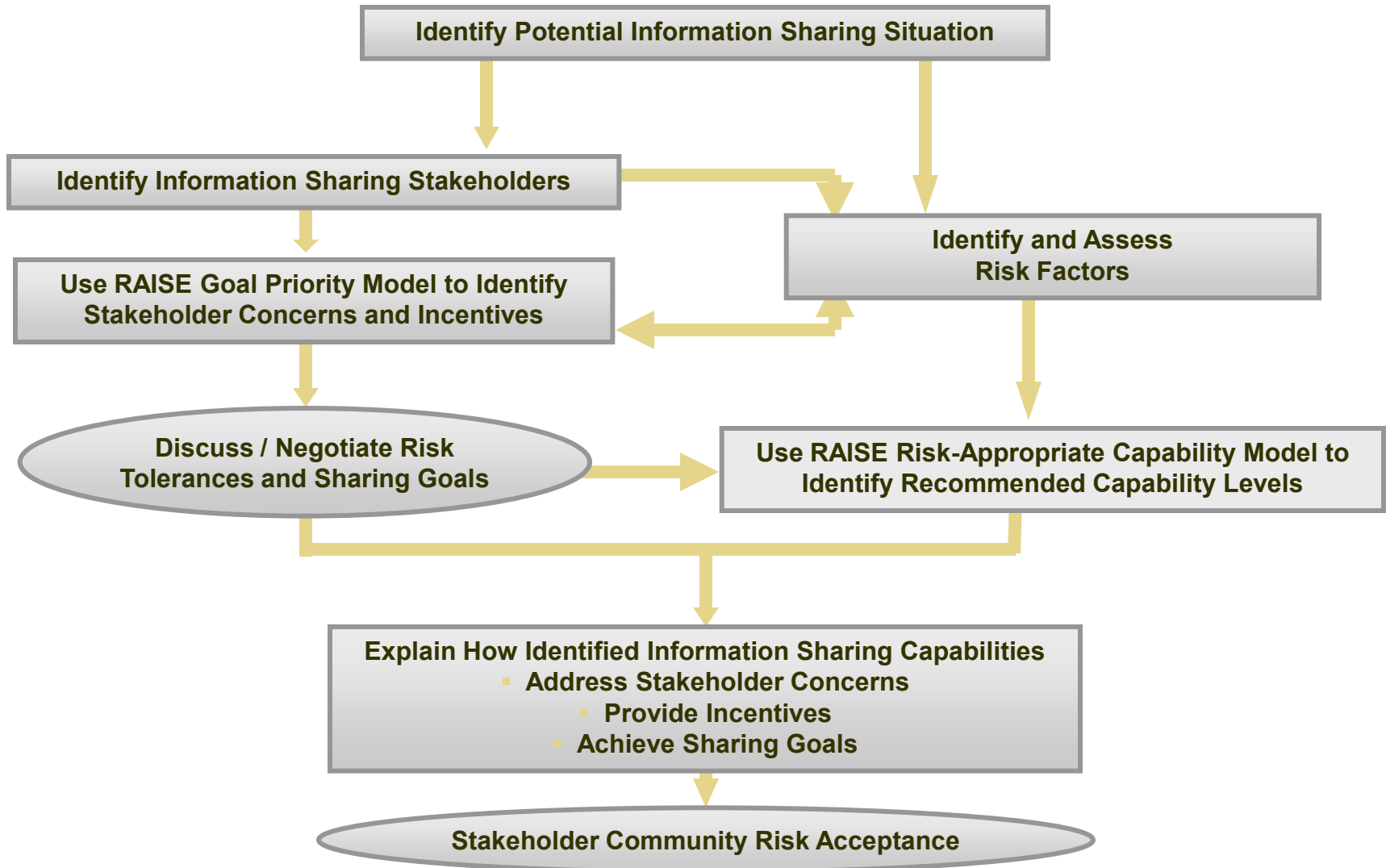
This Detailed Model Addresses Needs of Systems / Business Process Engineers:

- Explain how different products contribute to sharing
- Provide practical recommendations on enabling technologies ... or procedural work-arounds

RAISE Tool

- Access database application
- Proof-of-concept prototype
 - Structured information gathering (automated worksheets)
 - ❖ Describe information sharing situation (actual or prospective)
 - ❖ Assess stakeholder concerns and incentives
 - ❖ Assess risk factors
 - Implementation of Goal Priority model to assess relative importance of information sharing goals to different stakeholders
 - Implementation of *portions of* Risk-Appropriate Capability model to recommend capability levels to mitigate risks
 - ❖ Some portions of this model remain to be defined
 - ❖ Some defined portions of this model are not implemented in the tool ... it's a proof-of-concept
- Used in case studies

RAISE Process



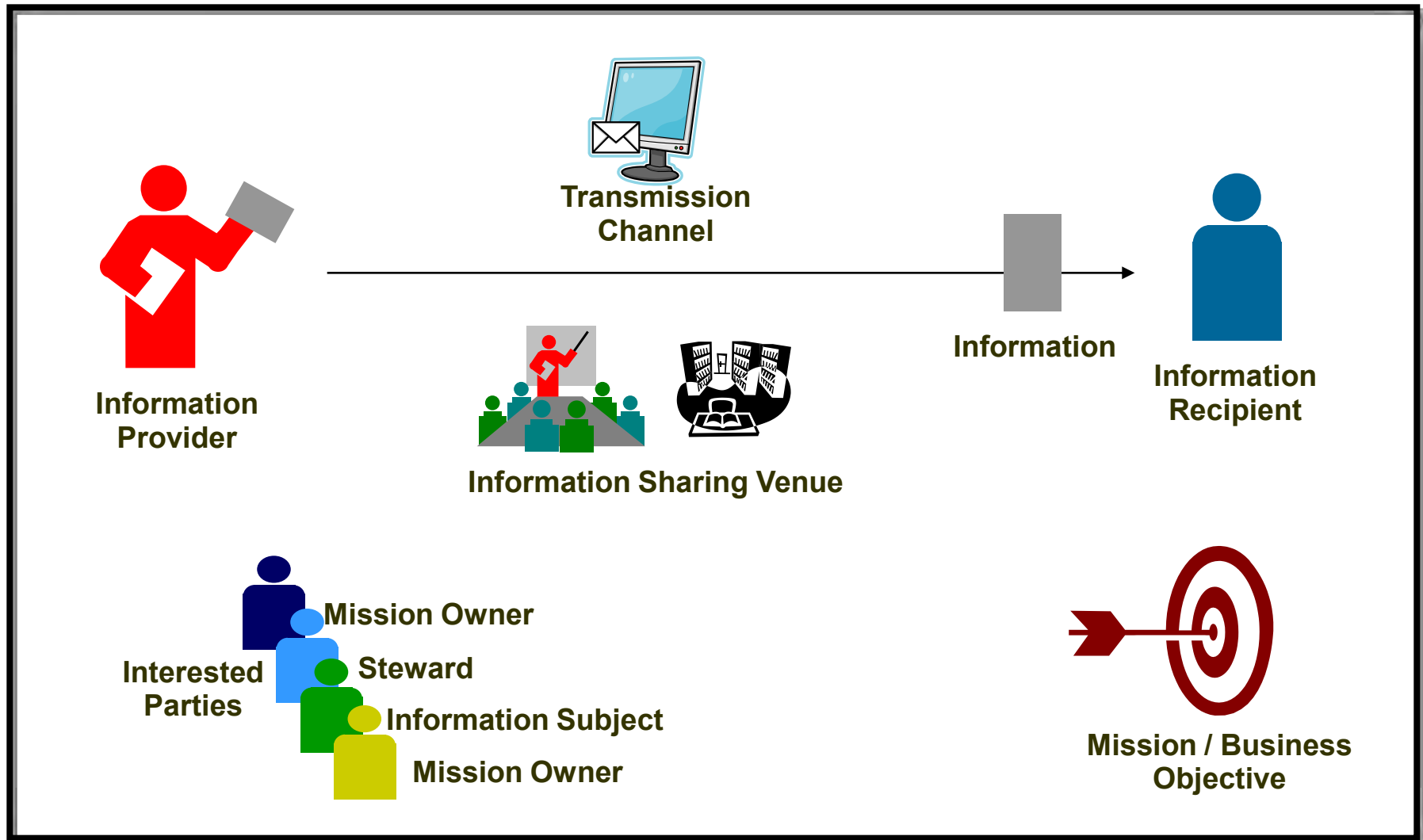
RAISE Status

- RAISE Version 1.0 is available for use
 - Complete framework
 - Complete Goal Priority model (fully documented and automated in proof-of-concept tool)
 - Most of Risk-Appropriate Capability model
 - ❖ Most capability recommendation functions fully documented
 - Use cases are needed to drive the definition of the remaining functions
 - ❖ A few capability recommendation functions automated in proof-of-concept tool
 - For further information, contact
 - ❖ Deb Bodeau (dbodeau@mitre.org, 781-271-8436)
 - ❖ Don Faatz (dfaatz@mitre.org, 315-838-2666)
 - ❖ Rich Graubart (rdg@mitre.org, 781-271-7976)
- RAISE is expected to evolve and mature
 - Validation and modification based on use cases



Backup / Additional Detail

Underlying Model of Information Sharing: Remain Technology-Neutral, Include Broad Range of Stakeholders





Key Assumption: Information Has Associated Terms of Use

- Assertions about restrictions and obligations that apply to any individual or organization that handles the information
 - How the information may / may not be used
 - With whom the information must / may / may not be shared
 - How the information must be protected
 - What accountability measures are needed for information handling actions
- Represented explicitly, implicitly, or indirectly
- Established by information creator, statutory or regulatory authority, contract or other agreement, and/or social convention

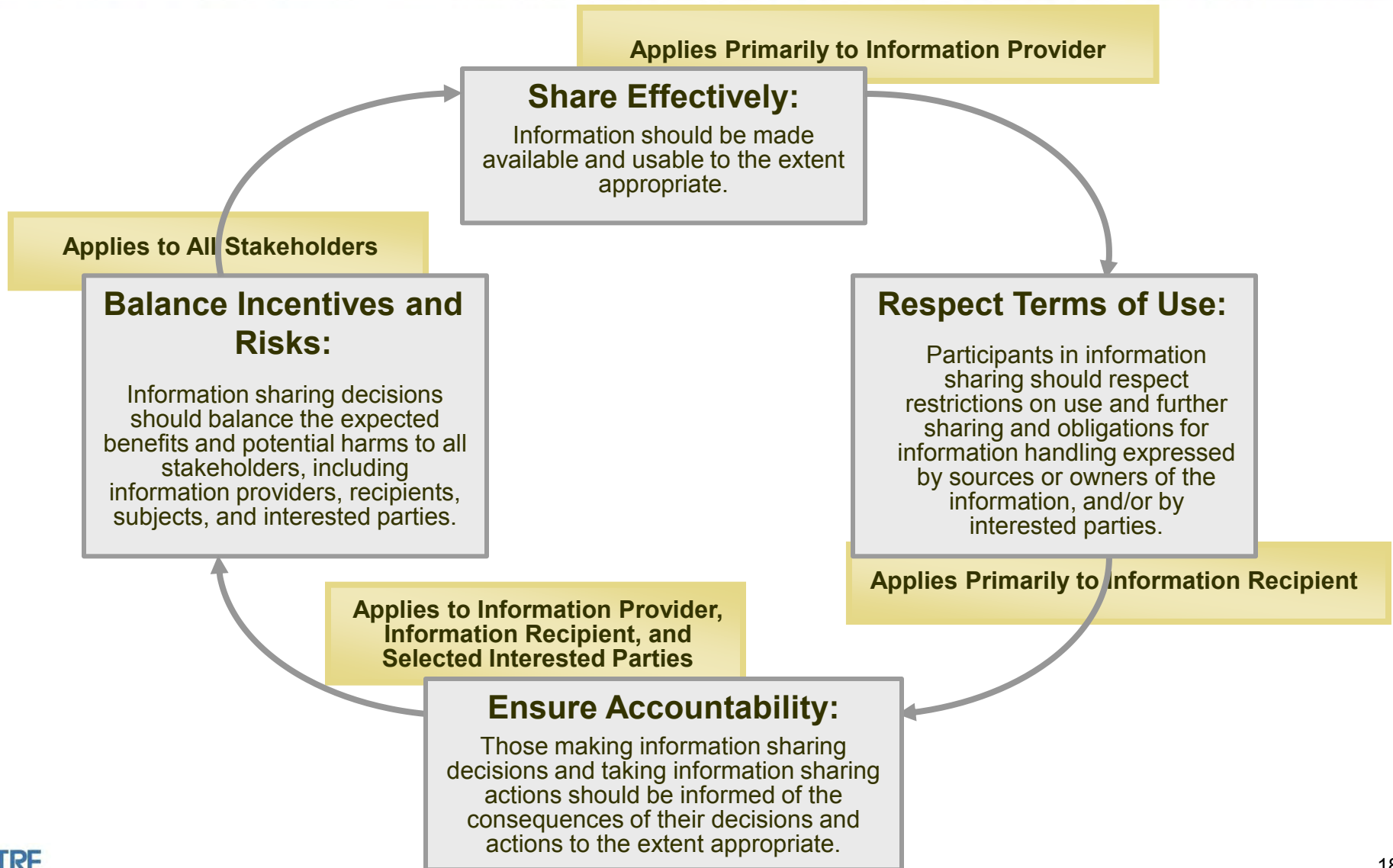


Key Assumption: Risk Arbitration Is Possible

- Information sharing stakeholders have different appetites and tolerances for risks
- If risks to all stakeholders can be articulated explicitly, and information sharing enablers are used in a risk-appropriate way, stakeholders can accept the residual risks or clearly state why sharing is unacceptable
 - Note: In some cases, sharing – or not sharing – is decided by *fiat* (e.g., law, regulation). The sharing decision authority is a *de facto* stakeholder, and the specific enablers that are used make a difference in the other stakeholders' acceptance of the decision.

All decisions to share or not share information incur potential risk. What varies is the degree of risk, who is impacted, and the type of risk.

RAISE Framework: Information Sharing Principles





RAISE Framework: Example of Principle, Goals, Capabilities

Balance Incentives and Risks:
 Information sharing decisions (whether, when, and how to share) should balance the expected benefits and potential harms to all stakeholders, including information providers, recipients, mission owners, stewards of information sharing venues, subjects, and other interested parties.

<p><i>Engage Stakeholders:</i> Stakeholders in information sharing – and in missions that are disserved by not sharing information – should be engaged to the extent appropriate to identify and manage risks.</p>
<p><i>Identify Potential Harms and Benefits:</i> The potential harms and benefits to stakeholders due to sharing – or to not sharing – information should be identified to the extent appropriate.</p>
<p><i>Identify Terms of Use:</i> The participants in information sharing should be able to identify the terms of use for the information to the extent appropriate.</p>
<p><i>Prevent Unintended Sharing:</i> Information that has not been explicitly shared should not be treated as shared.</p>

<ul style="list-style-type: none"> • Stakeholder Identification • Stakeholder Engagement at the Policy Level • Stakeholder Engagement at the Operational Level
<ul style="list-style-type: none"> • Specificity of Harm Identification • Specificity of Harm Assessment
<ul style="list-style-type: none"> • Specification of Terms of Use • Disambiguation of Terms of Use for Composite Information • Timing of Notification of Terms of Use
<ul style="list-style-type: none"> • Restriction of Requests for Information • Contamination Protection / Prevention

RAISE Framework: Capabilities and Examples of Enablers (1 of 4)

RAISE Framework			
Information Sharing Goals	Capabilities	Examples of Enabling Technologies and Processes	
Balance Incentives and Risks	Engage Stakeholders	<ul style="list-style-type: none"> Stakeholder Identification Stakeholder Engagement at the Policy Level Stakeholder Engagement at the Operational Level 	<ul style="list-style-type: none"> Balanced Scorecard Outreach processes
	Identify Potential Harms	<ul style="list-style-type: none"> Specificity of Harm Identification Specificity of Harm Assessment 	<ul style="list-style-type: none"> Standards for determining information sensitivity and quality (e.g., FIPS 199) Consequence assessment techniques (e.g., Analytic Hierarchy Process)
	Identify Terms of Use	<ul style="list-style-type: none"> Specification of Terms of Use Disambiguation of Terms of Use for Composite Information Timing of Notification of Terms of Use 	<ul style="list-style-type: none"> Languages for communicating and comparing terms of use (e.g., SPARCLE, Sharing Policy Language (SPL), Enterprise Privacy Authorization Language (EPAL), rule-based policy languages) Resolution of terms of use for aggregated or combined data (e.g., policy composition logics, Data-Purpose Algebra) Notice prior to sharing
	Prevent Unintended Sharing	<ul style="list-style-type: none"> Restriction of Requests for Information Contamination Protection / Prevention 	<ul style="list-style-type: none"> Trusted intermediary to screen requests (e.g., ISAC) Fine-grained controls

RAISE Framework: Capabilities and Examples of Enablers (2 of 4)

RAISE Framework		
Information Sharing Goals	Capabilities	Examples of Enabling Technologies and Processes
Share Effectively	Share Predictably	<ul style="list-style-type: none"> • Languages and mechanisms for communicating and comparing trust in participants • Data sharing agreements • Indexing and catalog publication tools
	Share Dynamically	<ul style="list-style-type: none"> • Dynamic Search Discovery • Dynamic Determination of Authorization / Access Privileges
	Authorize Initial Disclosure	<ul style="list-style-type: none"> • Authorization Process • Authorization Timing • Redaction
	Make Information Understandable	<ul style="list-style-type: none"> • Content Transformation • Structural Transformation
	Ensure Quality	<ul style="list-style-type: none"> • Quality Specification • Quality Assurance
		<ul style="list-style-type: none"> • Information sensitivity / releasability review prior to sharing • Security Guards • Declassification policies • Dirty word checkers / filtering tools • Hidden data detection tools and processes • HIPAA-related de-identification Anonymization tools and k-anonymity techniques • Obfuscation tools
		<ul style="list-style-type: none"> • Metadata tagging • Ontologies • Data and vocabulary standards
		<ul style="list-style-type: none"> • Information quality review processes (including non-security-related redaction) • Data correction processes and controls • Integrity assurances (e.g., checksums, digital signatures) • Vocabularies and standards for defining / ensuring information quality • Deception analysis tools



RAISE Framework: Capabilities and Examples of Enablers (3 of 4)

RAISE Framework			
Information Sharing Goals	Capabilities	Examples of Enabling Technologies and Processes	
Respect Terms of Use for Information	Authorize Additional Sharing	<ul style="list-style-type: none"> • Additional Sharing / Onward Transfer Authorization Process 	<ul style="list-style-type: none"> • Notice / approval process prior to additional sharing • Super-sticky release mechanisms
	Provide Corrections	<ul style="list-style-type: none"> • Upstream Correction Process • Downstream Correction Process 	<ul style="list-style-type: none"> • Processes and procedures
	Enable Revocation	<ul style="list-style-type: none"> • Recipient Participation in Revocation • Revocation Due to Security Spillage • Revocation Due to Poor Quality • Revocation Due to Intellectual Property Concerns 	<ul style="list-style-type: none"> • Processes and procedures for revocation of sharing • Data spillage detection and remediation tools and procedures
	Protect Information	<ul style="list-style-type: none"> • Information Protection 	<ul style="list-style-type: none"> • Security programs
	Restrict Uses	<ul style="list-style-type: none"> • Usage Restriction 	<ul style="list-style-type: none"> • DRM tools • Trusted intermediary to control information
	Dispose of Information	<ul style="list-style-type: none"> • Disposal Process • Disposal Accountability • Disposal Completeness 	<ul style="list-style-type: none"> • Data expiration tools • Assured data destruction tools

RAISE Framework: Capabilities and Examples of Enablers (4 of 4)

RAISE Framework			
Information Sharing Goals	Capabilities	Examples of Enabling Technologies and Processes	
Ensure Accountability	Give Credit	<ul style="list-style-type: none"> • Credit Mechanism 	<ul style="list-style-type: none"> • Financial payment / monetization • Citation (e.g., in publications) • Digital watermarking, steganography, or other embedding to ensure that owner / provider / source is credited • Access counters (e.g., on Web pages)
	Steward Sharing Venues	<ul style="list-style-type: none"> • Sharing Venue Policies • Enforcement of Sharing Venue Policies • Value-Added Stewardship 	<ul style="list-style-type: none"> • Stewardship policies and procedures • Consistency checking
	Provide Feedback	<ul style="list-style-type: none"> • Feedback Mechanism 	<ul style="list-style-type: none"> • Rating systems (e.g., on Wikis, blogs, and message boards) • Reputation systems
	Monitor Information Sharing Actions	<ul style="list-style-type: none"> • Monitoring Processes • Identification of Events or Actions to Monitor • Confidence in Monitoring 	<ul style="list-style-type: none"> • Logging / audit of information sharing activities • Immutable audit trail • Cross-domain audit
	Redress Violations	<ul style="list-style-type: none"> • Redress Processes 	<ul style="list-style-type: none"> • Incident response processes • Institution-internal redress processes • Legal, regulatory, or social sanctions

RAISE Framework: Example of Definitions of Capability Levels

Information Sharing Goal: Authorize Disclosure		
Capability	Achievement Levels / Values	Examples
Redaction: How completely and effectively is information that has not been authorized for disclosure or release as part of information sharing removed from a shared information object?	None – No attempt is made to identify and remove information that is not immediately apparent to the reviewer.	None
	Low – Unstructured processes to identify and remove information that is not immediately apparent are applied.	In Microsoft Office, the reviewer edits the document properties, accepts all changes, and saves the file as new.
	Medium – Partially structured processes are applied. Tools are matched to some types of shared information objects; if no tools are available for a given object type, ad-hoc analysis is performed.	Hidden data detection tools for documents
	High – Structured processes are applied. Sophisticated tools are matched to each type of information object that is shared.	Steganographic detection tools for images



RAISE Goal Priority Model: Determine the Relative Importance of Information Sharing Goals

**Stakeholder
Concerns**

<p>Balance Incentives and Risks: Engage stakeholders. Identify potential harms and benefits. Identify terms of use. Prevent unintended sharing.</p>	<p>Share Effectively: Share predictably. Share dynamically. Authorize initial disclosure. Make information understandable. Ensure quality.</p>	<p>Respect Terms of Use: Authorize additional sharing. Enable revocation. Provide corrections. Restrict uses. Protect information. Dispose of information.</p>	<p>Ensure Accountability: Give credit. Provide feedback. Steward sharing venues. Monitor information sharing actions. Redress violations.</p>
--	---	---	--

<p>Information Sharing Method</p> <ul style="list-style-type: none"> • Form of shared information • Method of providing information • Provider control / specificity • Provider-recipient interaction 	<p>Stakeholder Relationships</p> <ul style="list-style-type: none"> • Stakeholder trust relationships • Stakeholder power relationships • Stakeholder authorizations for information 	<p>Information & Contextual Attributes</p> <ul style="list-style-type: none"> • Sensitivity • Criticality • Structure • Transience / Persistence
--	--	---



RAISE Goal Priority Model Requires Identification of Stakeholders and Assessment of Their Concerns

Identify Potential Information Sharing Situation

- Who?
 - Information provider
 - Information recipient
 - What?
 - Information (general description)
 - [About whom? information subject]
 - When and where?
 - Under what circumstances the information is shared – at least a general description
 - Why?
 - Mission / business objective
 - [Legal / regulatory requirement]
 - How?
 - [Following what process, in what form, using what technologies]
- [topics in brackets may not be applicable to some information sharing situations]

Identify Information Sharing Stakeholders

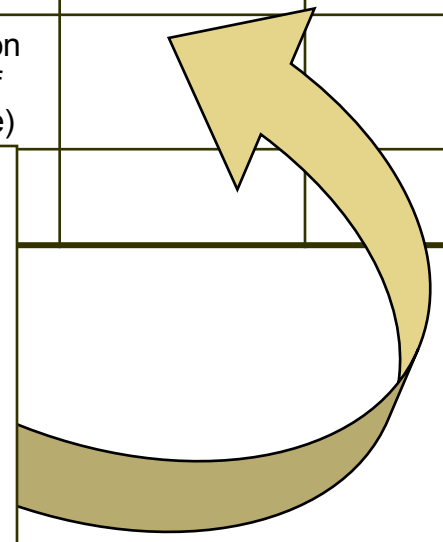
- Information provider
- Information recipient
- Interested parties
 - Stewards of information sharing venues
 - Entities in the same sector as the information provider or recipient
 - Information subjects
 - Beneficiaries of mission / business process supported by information sharing
 - Representatives of public interests (e.g., elected officials, regulators)

Use Top-Level RAISE Model to Identify Stakeholder Concerns

Stakeholder	Concerns / Potential Harm Due to Sharing	Incentives to Share / Concerns if No Sharing
Information Provider		
Information Recipient		
Information Subject (if applicable)		

Concerns for

- Mission ineffectiveness or failure
- Costs (resources used or committed)
 - Information management
 - Meeting obligations
 - Financial / opportunity costs
- Non-financial impacts
 - Repercussions of failure to meet obligations
 - Damage to reputation (loss of good will, loss of trust)





Case Study: Sharing CIP Incident Information (Retrospective Example circa 1999)

- National Infrastructure Protection Center (NIPC) is intended to provide
 - Near real-time notification of threatened or actual malicious actions against critical infrastructure
 - Evidence of coordinated attacks against U.S. national interests
 - Timely, accurate, and actionable warnings to critical infrastructure owners and operators
- NIPC needs critical infrastructure owners and operators to provide incident information
 - Initial reports within 30 minutes of detection
 - Follow-up report within 6 hours of detection
 - Final report within 60 days of incident

RAISE Tool: Main Menu

Risk-Appropriate Information Sharing Enablers (RAISE) Tool - Main Menu

Data Entry Worksheet: Characterizing the Information Sharing
Situation

Data Entry Worksheet: Assessing Stakeholder Concerns

Definitions: Assessment Factors and Assessment Values

Framework: Principles, Goals, and Capabilities

Definitions: Key Vocabulary

Reports



RAISE Tool: Data Entry for CIP Case Study – General Background

Characterizing the Information Sharing Situation: General Background

Situation

Summary Description (Describe the information sharing situation - what individuals and/or organizations provide information, to what individuals and/or organizations, what information is shared, how, and for what purposes.)

Entities operating critical infrastructure in all sectors, electric power, information and communication, transportation, emergency law enforcement services, emergency fire service, oil and gas production and storage, banking and finance, water supply, public health services, continuity of government services will incidents to the National Infrastructure Protection Center (NIPC). Incident reports will be used by intelligence analysts to identify sign of an attack on the United States critical infrastructure. This effort is part of the National

Sharing Status (Does the information sharing situation currently exist? Or is it planned or proposed? If a sharing agreement, Memorandum of Understanding, or interface control document (ICD) exists, provide the reference.)

This is a planned sharing situation. No agreements currently exist.

Sharing Drivers (Identify the reasons for the information sharing situation. These include the missions or business objectives that the sharing does or would support, as well as any regulatory, legal, policy, or contractual mandates to share information.)

Presidential Decision Directive 63, Critical Infrastructure Protection, and establishment of the NIPC are drivers for this information sharing situation. The shared information is needed by NIPC to perform its indications and warning function.

Criticality of Mission (How important is the mission which the sharing is intended to support - on a broad scale [e.g., to national security, homeland security, or public health and safety] and/or on an enterprise or sector scale [e.g., to the information recipient or to interested parties]?)

Broad scale criticality Narrow scale criticality

To stakeholder or set of	None	No harm will occur if this mission is not accomplished
Low	Failure to accomplish this mission will have noticeable, but not significant, impacts on national security, homeland security, or public health and safety	
Medium	Failure to accomplish this mission will have significant impacts on national security, homeland security, or public health and safety	
High	Failure to accomplish this mission will have highly significant impacts on national security, homeland security, or public health and safety	

RAISE Tool: Data Entry for CIP Case Study – Stakeholder Concerns

Information Provider Concerns

Provider Name

Concerns if Information Is Shared

(Provide amplifying discussion as necessary. Assess the level of concern (VL-VH), using the scales below, or mark as not applicable. Also indicate whether the concern is related to the information (I), the information sharing method (M), or both.)

ID	Definition	Description	Assessment	Related to
PS1	Damage to information provider's future mission capabilities if information is improperly disclosed:	Provider may lose customers. Competitors	Medium	Information
PS2	Potential disclosure of sensitive information about provider missions, activities, and	Competitors may gain advantage	Very Low	Information
PS3	Liability if sharing violates terms of use for information:	Provider owns information and sets terms of use	None	Information
PS4	Liability for results of recipient decisions / actions based on shared information:		None	Information
PS5	Mistrust / loss of reputation if shared information is of inadequate quality:		None	Information

Record: of 10

Incentives for Sharing Information / Concerns if Information Is Not Shared

(Provide amplifying discussion as necessary. Assess the level of concern (VL-VH), using the scales below, or mark as not applicable.)

ID	Definition	Description	Assessment
PN3	Efficiencies due to predictable sharing. Costs of responding on an ad-hoc basis to requests for		None
PN4	Increased support for provider organization. Budget cuts or lack of partnerships, if information		None
PN5	Enhanced reputation and recognition. Lack of recognition for expertise / achievements:		None
PN6	Realistic expectations of provider's missions and capabilities. Potential misperception of provider		None
PN7	Synergy between provider and recipient or overarching missions. Lost opportunity for mission	High quality warnings based on shared	Very Low

Record: of 7

RAISE Tool: Report Menu

RAISE Report Menu

Summary Reports

Preview Summary Report (P,R,V,M)

Preview Summary Report (S,O,X)

Preview Provider Report

Preview Recipient Report

Preview Mission Owner Report

Preview Data Owner Report

Preview Info Subject Report

Preview Steward Venue Report

Preview Other Interested Party Report

Worksheet

General Background Section

Provider - Recipient Information

Information Subject Information

Mission Owner Information

Data Owner Information

Other Interested Party Information

Information Characteristics

Sharing Method

Initial Stakeholder Concerns

Recommended Capability Levels



RAISE Tool: Example of Report on Relative Importance of Information Sharing Goals

RAISE Report: Relative Importance of Information Sharing Goals to Information Provider, Recipient, Sharing Venue Steward, and Mission Owner

Goal	Importance to Provider	Importance to Recipient	Importance to Venue Steward	Importance to Mission Owner
------	------------------------	-------------------------	-----------------------------	-----------------------------

Engage stakeholders	Medium	Medium	None	High
Identify potential harms and benefits	High	Medium	None	High
Identify Terms of Use	None	Medium	None	Medium
Share predictably	Low	None	None	Medium
Share dynamically	Very Low	Medium	None	Medium
Authorize initial disclosure	High	Medium	None	High
Make information understandable	Very Low	None	None	Medium
Ensure quality	Very Low	None	None	-
Authorize additional sharing	High	None	None	None
Prevent unintended sharing	High	None	None	Medium
Enable revocation	High	High	None	Medium
Provide corrections	Very Low	None	None	-
Restrict uses	None	High	None	-
Protect information	High	None	None	Medium
Dispose of information	High	None	None	None
Give credit	None	None	None	None



RAISE Tool: Example of Recommended Capability Levels

RAISE Report: Recommended Capability Level

Goal

Capability

Recommended level

Share predictably

Predictability of Publication / Distribution: To what extent can the information recipient predict whether and how the information provider will publish or distribute information?

Medium: The provider states that information will be published or distributed under specific circumstances (e.g., at specific time intervals) and/or in specific ways. The recipient has grounds for believing the provider's assertion (e.g., observation of prior sharing, trusted third party vouching for provider).

Data Sharing Negotiation / Agreement: To what extent does the information provider define or negotiate, and agree to, a statement of what information will be shared, how, how often and/or under what circumstances, and with what terms of use?

Medium: Partially structured processes are used to establish what information will be shared predictably. Those processes include provider definition of roles and responsibilities for determining or negotiating what information will be shared, how often and/or under what circumstances, and with what terms of use. The resulting agreement is documented. The shared information is characterized in terms of its content.

Case Study: Sharing Neuroimaging

- Researchers at one institution perform a study to produce a fine-grained, time-based anatomic atlas of Alzheimer's progression
 - Four-year study of twenty-five patients
 - Each patient receives four structural MRIs per year
- Information sharing scenario
 - Collaboration with a colleague at another institution who specializes in analysis that may yield important results

Ken Smith, et. al. "Enabling the Sharing of Neuroimaging Data Through Well-Defined Intermediate Levels of Visibility," *NeuroImage* 22 (2004)



Neuroimagery Sharing Case Study: Stakeholders

- **Information Provider:** Principal Investigator of Alzheimer's progression study
- **Information:** 400 structural MRIs of the information subject, associated metadata, and patient medical histories
- **Information Recipient:** Collaborator with specialized analysis techniques
- **Information Subject:** The 25 patients participating in the study
- **Interested Party:**
 - Mission Owner: NIH, as representative of overall mission of improving healthcare
 - Data Owner: N/A
 - Other: Health care providers, current and future Alzheimer's patients
- **Information Sharing Context:** The information will be provided to the collaborator as digital data on DVDs. The collaborator will load the digital data onto her research computer systems. Data is not anonymized.

Neuroimaging Sharing Case Study: Stakeholder Concerns (1 of 2)

Stakeholder	Adverse Consequences of Sharing	<i>Incentives to Share / Adverse Consequences of Not Sharing</i>
Information Provider (researcher who has collected imagery)	1) Data reused without proper citation [Low] (PS7: Loss of credit / intellectual properties rights for shared information) 2) Shared data violates privacy laws [Moderate] (PS3: Liability if sharing violates terms of use for information)	3) Lost opportunity for building reputation [Moderate] (PN5: <i>Enhanced reputation and recognition / Lack of recognition for expertise / achievements</i>) 4) Lost opportunity for research synergy [Low] (PN7: <i>Synergy between provider and recipient or overarching missions / Lost opportunity for mission synergy</i>)
Information Subject (Images, metadata, medical history)	5) Information subject is denied coverage after data accessed by insurer [Moderate] (SS4: Information shared with unauthorized secondary recipient in a manner that is harmful to subject and was not agreed to by subject) 6) Data used for purpose not agreed to by subject [Moderate] (SS6: Information used for a purpose to which the subject has not consented, leading to perceived or actual adverse effects on the subject)	7) Incorrect/inadequate treatment [Low] (SN1: <i>Timely and well-informed services provided by the recipient to the subject / Decisions or actions taken by the recipient, based on the absence of relevant data, that adversely affect the subject (e.g., denial of service)</i>)

Neuroimagery Sharing Case Study: Stakeholder Concerns (2 of 2)

Stakeholder	Adverse Consequences of Sharing	<i>Incentives to Share / Adverse Consequences of Not Sharing</i>
Information Recipient (Collaborator)	8) Shared data violates privacy laws – legal/financial penalties [Moderate] (RS2: Liability / consequences if sharing violates terms of use for information (e.g., sanitization of data spillage))	9) Lost opportunity for building reputation [Moderate] (RN3: <i>Enhanced reputation and recognition due to use of shared information / Lack of recognition for expertise / achievements</i>) 10) Lost opportunity for research synergy [Low] (RN4: <i>Synergy between recipient and provider or overarching missions / Lost opportunity for mission synergy</i>)
Interested Party (health care providers, current and future patients, NIH)	11) Unwarranted optimism based on incorrect release [Low] (MS2: Damage to mission if decisions are based on inadequate-quality or misunderstood information) 12) Other researchers do not pursue promising lines of investigation based on incorrect publication [Low] (MS2: Damage to mission if decisions are based on inadequate-quality or misunderstood information)	13) Lost opportunity for understanding Alzheimer’s progression and treatment development [Moderate] (MN1: <i>Improved mission effectiveness and/or business efficiency / Impacts to overarching mission / business objectives</i>)


RAISE Risk-Appropriate Capability Model: Risk Factors Underlie Concerns



Differences in Authorization



Information Provider **Organizational, Power, and Trust Relationships** **Information Recipient**

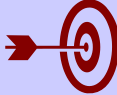


Sensitivity
Opaqueness / Transparency
Type (form, content)
Actual Quality

information





Steward Control
Steward Value-Added




Criticality of Mission
(broad-scale, stakeholder-specific)
Criticality of Sharing to Mission
Quality Requirements
(timeliness, other)

mission or business objective

Information Structure
Interactivity
Transience



information sharing venue transmission channel



RAISE Risk-Appropriate Capability Model: Use to Select Sharing Capabilities to Mitigate Risk

- Sharing Capabilities are related to Sharing Goals
 - A disclosure process is an enabler of the Authorize Initial Disclosure goal
- Use of Sharing Capabilities is related to Risk Level
- Risk Level is a function of relevant Risk Factors
- Therefore, use of Sharing Capabilities is a function of relevant Risk Factors
 - A disclosure process can be Non-existent, Unstructured, Partially Structured, or Structured depending on the level of risk it is intended to mitigate
 - Risk level associated with the type of disclosure process is a function of provider-recipient trust, information quality, and provider-recipient authorization difference

Provider-Recipient Trust	Max (Information quality requirements, Provider-Recipient Authorization Difference)			
	High	Medium	Low	None
...
Medium	Medium – Partially structured process	Medium – Partially structured process	Low – Unstructured process	Low – Unstructured process
High	Low – Unstructured process	Low – Unstructured process	Low – Unstructured process	None – Individual judgment
Very High	Low – Unstructured process	Low – Unstructured process	None – Individual judgment	None – Individual judgment



Example: Mapping Stakeholder Concerns to Information Sharing Goals

- Goal: Engage Stakeholders

- PN5: *Enhanced reputation and recognition / Lack of recognition for expertise / achievements*
- PN7: *Synergy between provider and recipient or overarching missions / Lost opportunity for mission synergy*
- SN1: *Timely and well-informed services provided by the recipient to the subject / Decisions or actions taken by the recipient, based on the absence of relevant data, that adversely affect the subject*
- RN3: *Enhanced reputation and recognition due to use of shared information / Lack of recognition for expertise / achievements*
- RN4: *Synergy between recipient and provider or overarching missions / Lost opportunity for mission synergy*
- MN1: *Improved mission effectiveness and/or business efficiency / Impacts to overarching mission / business objectives*

- Goal: Make information understandable

- MS2: Damage to mission if decisions are based on inadequate-quality or misunderstood information

- Goal: Authorize initial disclosure

- PS3: Liability if sharing violates terms of use for information
- RS2: Liability / consequences if sharing violates terms of use for information
- MS2: Damage to mission if decisions are based on inadequate-quality or misunderstood information

- Goal: Restrict uses

- SS6: Information used for a purpose to which the subject has not consented, leading to perceived or actual adverse effects on the subject
- SS4: Information shared with unauthorized secondary recipient in a manner that is harmful to subject and was not agreed to by subject

- Goal: Give credit

- PS7: Loss of credit / intellectual properties rights for shared information



Neuroimagery Sharing Case Study: Apply Capabilities to Address Concerns and Meet Goals (1 of 2)

Capability for “Authorize Initial Disclosure” goal – authorization process

- Level of authorization process (None, Unstructured, Partially Structured, Structured)
 - Determined by Max (information quality requirement, authorization difference) and provider-recipient trust
 - ❖ Quality requirement: Medium (Inadequate information quality will prevent the consulted colleague providing help)
 - ❖ Authorization difference: None
 - ❖ Provider-recipient trust: High (Trust is a function of prior experience, cooperative / competitive relationship, shared cultural / mission understanding, and conflicting mandates)

Provider-Recipient Trust	Max (Information quality requirements, Provider-Recipient Authorization Difference)			
	High	Medium	Low	None
...
Medium	Medium – Partially structured process	Medium – Partially structured process	Low – Unstructured process	Low – Unstructured process
High	Low – Unstructured process	Low – Unstructured process	Low – Unstructured process	None – Individual judgment
Very High	Low – Unstructured process	Low – Unstructured process	None – Individual judgment	None – Individual judgment

Neuroimagery Sharing Case Study: Apply Capabilities to Address Concerns and Meet Goals (2 of 2)

Capability for “Authorize Initial Disclosure” goal – authorization process

- Timing of process (Post hoc, Immediate, Deliberate, A priori)
 - Determined by nature of sharing (dynamic, predictable), information quality requirements, and criticality of sharing to mission
 - ❖ Nature of sharing: Predictable
 - ❖ Information quality requirements: Medium
 - ❖ Criticality to mission: Medium (PI will be significantly less able to get important results if information is not shared with consulting colleague)

Nature of Sharing	Information quality requirements – timeliness	Criticality of Sharing to Mission			
		None	Low	Medium	High
Dynamic (a priori is not an option)	None	none (N/A)	deliberate	deliberate	immediate
	Low	deliberate	deliberate	deliberate	immediate
	Medium	deliberate	deliberate	immediate	immediate
	High (reflects the world in near real time)	deliberate	deliberate	immediate	post hoc
Predictable	N/A	deliberate	deliberate	deliberate	a priori



Neuroimagery Sharing Case Study: Use of Risk-Appropriate Capability Model Produces Recommendation for Disclosure Authorization

- Use an unstructured deliberate process to authorize disclosure
 - Unstructured: Individual judgment is applied, based on organizational guidance regarding the Terms of Use.
The PI applies individual judgment, checking that the sharing is consistent with the Privacy Notice to which the information subjects consented.
 - Deliberate: The decision is made with enough time for human deliberation and consultation.
PI has time to consult with his/her institution's ethics / privacy committee before sharing the information, if any doubts about the legitimacy of the sharing arise.